GTA Georgia Technology Authority	**Georgia Technology Authority**	
Title:	**Wireless and Mobile Computing**	
PSG Number:	SS-08-039.01	**Topical Area:** Security
Document Type:	Standard	**Pages:** 2
Issue Date:	3/31/08	**Effective Date:** 3/31/08
POC for Changes:	GTA Office of Information Security	
Synopsis:	Establishes minimum security requirements for wireless network implementation.	

PURPOSE

Wireless and mobile computing technologies offer network users benefits such as portability, flexibility and increased productivity. As employees connect remotely to the state networks, these entry points and data transmission modes increase the risks and vulnerabilities to agency internal networks and must be properly secured.

This standard establishes the minimum requirements for implementing wireless network access.

SCOPE; ENFORCEMENT; AUTHORITY; EXCEPTIONS

See Enterprise Information Security Charter (policy)

STANDARD

Prior to implementing wireless and mobile technologies, agencies shall be aware of the technical and security implications associated with these technologies and assess the risks to ensure appropriate steps are taken to mitigate these risks.

To mitigate the security risks associated with wireless and mobile computing, system owners shall protect the internal systems by implementing the strongest, most appropriate security controls for encryption, user authentication and end-point protection mechanisms. Anti-virus protection and perimeter controls shall be properly configured and port openings shall be secured, restricted and monitored.

Agencies shall create a Wireless LAN (WLAN) Implementation Plan (as described in the WLAN Implementation Guideline) that adequately addresses the following areas of concern:

- Remote access, wireless access, and mobile computing policies and procedures
- WLAN architecture and implementation
- Configuration and security of access points
- Encryption and encryption keys
- Integration of wireless network to wired network (VPN)
- Security of data transmissions between wired and wireless networks
- Logical and physical protection of wireless/mobile/end-point devices
- Logical and physical protection of stored data in transit.

- Change management and configuration control
- Audit/monitoring
- Penetration tests and vulnerability assessments
- Malicious code protection and Incident handling
- Security Awareness and Training

Agencies shall conduct periodic reviews to ensure that the wireless network and remote access technologies are utilized in a secure manner and in compliance with all applicable security requirements and standards.

The deployment and operation of open, unsecured wireless network access technology is prohibited.

RELATED ENTERPRISE POLICIES, STANDARDS, GUIDELINES

- Remote Access (Policy)
- Remote Access (Standard)
- WLAN Implementation (Guideline)
- Use of Cryptography (Policy)
- Use of Cryptographic Controls (Standard)

REFERENCES

- NIST SP 800-48, Wireless Network Security
- NIST SP 800- 28 Guidelines on Active Content and Mobile Code
- NIST SP 800-19 Mobile Agent Security
- NIST SP 800-97 Establishing Wireless Robust Security Networks

TERMS AND DEFINITIONS

Remote Access - The ability of an organization's users to access its non-public computing resources from locations outside the organization's security boundaries.

Telework or telecommute - The ability of an organization's employees and contractors to conduct work from locations other than the organization's facilities.

Mobile Computing - A generic term describing one's ability to use technology 'untethered', that is not physically connected, or in remote or mobile (non static) environments.

Note: The PSG number was changed from S-08-039.01 on September 1, 2008.